TR CMS 101:2015 und TR CMS 100:2015

TÜV Media

Compliance-Management-Systeme – Standard und Leitfaden

TÜVRheinland®
Genau. Richtig.

Herausgegeben von TÜV Rheinland Cert GmbH, Köln

TÜV Rheinland Group

Autoren: Walter Schlegel, Dipl.-Ing., Technischer Betriebswirt
Rainer Vieregge, Dipl.-Ing.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie. Detaillierte bibliografische Daten sind im Internet unter http://dnb.d-nb.de abrufbar.

ISBN 978-3-8249-1974-1

www.tuev-media.de

Gesamtinhaltsverzeichnis

Teil 1

TR CMS 101:2015
Standard für Compliance-Management-Systeme (CMS)

des TÜV Rheinland, Köln

TÜVRheinland®
Genau. Richtig.

Vorwort

Die Führung ist für die Einrichtung, Aufrechterhaltung und ständige Verbesserung eines Management-Systems zur Erfüllung der Compliance-Anforderungen verantwortlich. Als Querschnittsthema betrifft Compliance alle Bereiche und Funktionen einer Organisation. Compliance-Maßnahmen erfolgen nicht isoliert, sondern müssen in die administrativen und operativen Abläufe der Organisation integriert werden. Dies erfordert eine systematische Herangehensweise, um die Erfüllung der Compliance-Anforderungen in der gesamten Organisation zu erreichen.

Angesichts der Bedeutung von Compliance und der möglichen Folgen von Verstößen gegen Compliance-Anforderungen handelt es sich beim Compliance-Management-System um ein eigenständiges Management-System. Das Compliance-Management-System weist Berührungspunkte zu anderen Management-Systemen und Regelwerken auf (z. B. Corporate Governance, Risikomanagement, Qualitätsmanagement, Umweltmanagement, Informationssicherheitsmanagement, Betriebliches Kontinuitätsmanagement, Nachhaltigkeitsmanagement etc.).

Compliance-Anforderungen sind nicht statisch, sondern unterliegen häufigen Änderungen (z. B. aufgrund von gesetzlichen Änderungen, der Aufnahme neuer Tätigkeiten oder der Erstreckung von Aktivitäten in neue Regionen). Für die Realisierung und eine ständige Verbesserung des Compliance-Management-Systems ist ein iterativer Prozess erforderlich.

Das in Bild 1 dargestellte Compliance-Management-System ist mit anderen Management-Systemen kompatibel und folgt dem kontinuierlichen Verbesserungsprinzip, der Planen-Durchführen-Prüfen-Handeln-Methode (Plan-Do-Check-Act, PDCA-Zyklus).

Die Dokumentation des Compliance-Management-Systems ermöglicht dessen unabhängige Umsetzung und Aufrechterhaltung.

Aus der wirksamen Umsetzung und Aufrechterhaltung eines Compliance-Management-Systems und dessen Kommunikation innerhalb und außerhalb der Organisation ergeben sich für die Organisation zusätzliche Chancen. Das dadurch erzeugte Vertrauen bei Stakeholdern (z. B. Mitarbeitern, Kunden, Behörden, Gesellschaftern, Investoren) kann sich in nachhaltigeren Beziehungen auswirken (z. B. stärkere Kundenbindung, langfristige Geschäftsbeziehungen, höhere Motivation der Beschäftigten). Darüber hinaus kann die Organisation von niedrigeren Kosten für Korrekturmaßnahmen, besseren Finanzierungskonditionen, günstigeren Versicherungsprämien und einer größeren Reputation profitieren.

0 Einleitung

Dieser Standard zeigt in Anlehnung an den ISO 19600 Standard für Compliance-Management-Systeme die Grundelemente auf, die ein Management-System zur Erfüllung der für die Organisation anwendbaren Compliance-Anforderungen enthalten muss. Die konkrete Ausgestaltung und Umsetzung des Compliance-Management-Systems ist organisationsabhängig und liegt in der Verantwortung der Führung.

Die in diesem Zertifizierungsstandard aufgezeigten Elemente des Compliance-Management-Systems sind überprüfbar und nachweisbar, um festzustellen, ob und in welchen Punkten eine Organisation über ein Compliance-Management-System verfügt, das die in Kapitel 2 beschriebenen Ziele erfüllt. Compliance-Management-Systeme können organisationsspezifisch unterschiedlich strukturiert oder dokumentiert sein.

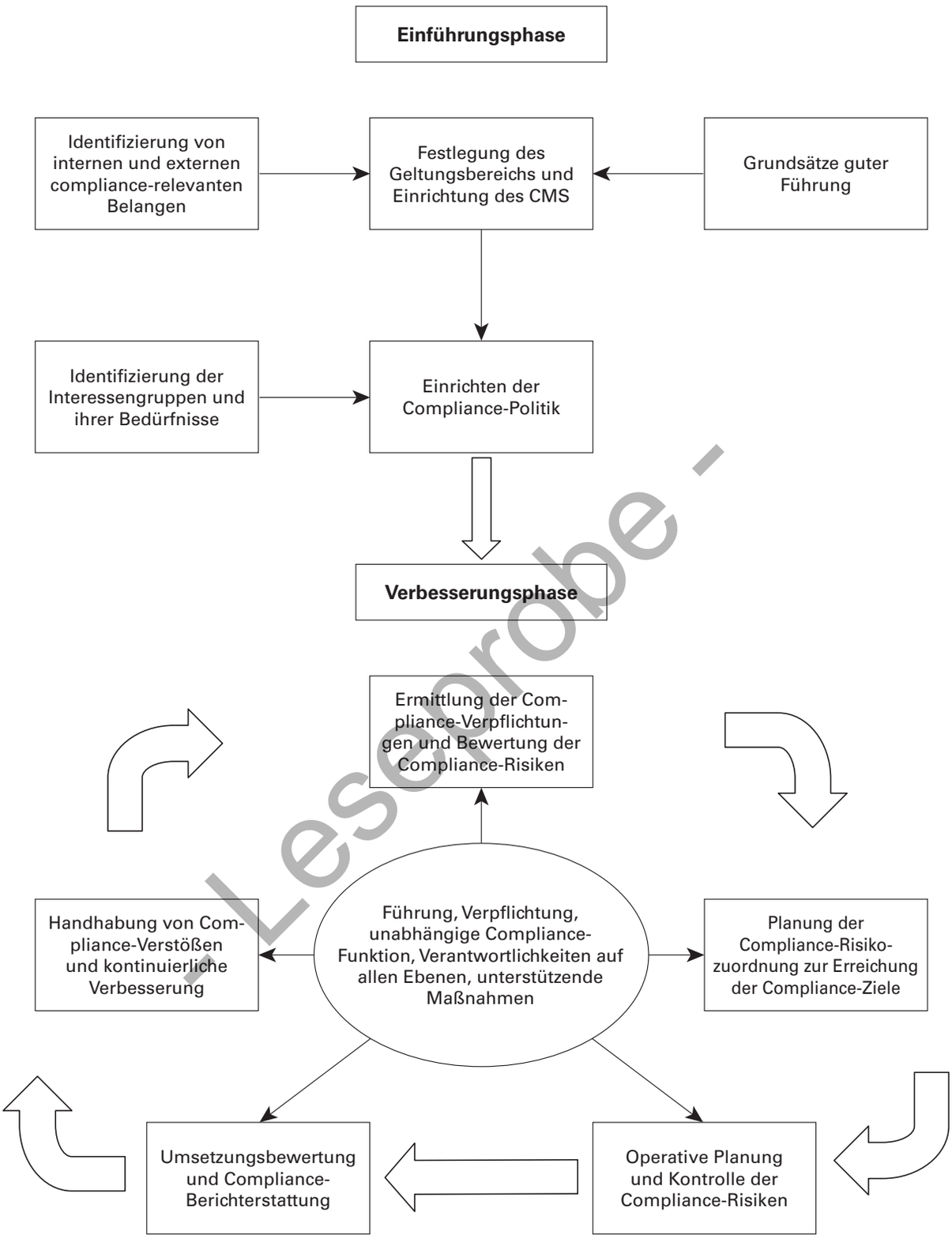

Bild 1: Visualisierung eines Compliance-Management-Systems (CMS)

Der Standard TR CMS 101:2015 für Compliance-Management-Systeme ermöglicht es, einer Organisation nach erfolgreicher Durchführung des Systemaudits in einem Zertifikat zu bescheinigen, dass sie nachweislich

a) ein Compliance-Management-System eingeführt hat und dieses aufrechterhält,

b) die Mindestanforderungen an ein Compliance-Management-System erfüllt und

c) in der Lage ist, präventive wie korrigierende Maßnahmen umzusetzen.

Mit der Zertifizierung des Compliance-Management-Systems wird keine Aussage darüber getroffen, dass die Organisation tatsächlich alle geltenden Compliance-Anforderungen erfüllt; die Durchführung des Zertifizierungsaudits stellt keine Beratung hinsichtlich der anwendbaren Regeln bzw. Rechtsberatung dar. Ein Zertifizierungsaudit bzw. eine Zertifizierung entbindet die Organisation nicht grundsätzlich von einer Haftung bei Organisationsverschulden oder Aufsichtspflichtverletzungen.

1 Anwendungsbereich

Der vorliegende Standard legt die grundlegenden Elemente fest, die zu einem Compliance-Management-System gehören. Er ist auf alle Organisationen unabhängig von ihrer Größe und Rechtsform sowohl national als auch international anwendbar.

Die Ausgestaltung und Verwirklichung des Compliance-Management-Systems wird beeinflusst durch

a) Größe und Struktur der Organisation, Art ihrer Tätigkeit,

b) Regionen, in denen die Organisation tätig ist,

c) bereitgestellte Produkte und Dienstleistungen,

d) Aufgaben in öffentlichen Einrichtungen,

e) angewendete Prozesse,

f) Umfeld, sich verändernde Erfordernisse,

g) spezifische Risiken der Organisation und

h) besondere Ziele der Organisation.

Elemente des Compliance-Management-Systems sind so festzulegen, dass sie nachgewiesen und überprüft werden können. Damit lässt sich feststellen, ob die Organisation über ein wirksames Compliance-Management-System verfügt.

2 Ziele des Compliance-Management-Systems

Ziel des Compliance-Management-Systems ist es, systematisch die Voraussetzungen in der Organisation dafür zu schaffen, dass Compliance-Vorgaben berücksichtigt und angewendet werden, Verstöße gegen Compliance-Anforderungen vermieden bzw. wesentlich erschwert und eingetretene Verstöße erkannt und behandelt werden können.

Teil 2

TR CMS 100:2015
Compliance-Leitfaden

des TÜV Rheinland, Köln

TÜVRheinland®
Genau. Richtig.

Zur Nutzung des Compliance-Leitfadens TR CMS 100:2015

Der Compliance-Leitfaden TR CMS 100:2015 richtet sich an Compliance-Beauftragte/Officer, Compliance-Auditoren, Unternehmen, Organisationen und Berater sowie an alle, die am Aufbau und an der Pflege eines Compliance-Management-Systems (CMS) beteiligt sind.

Er interpretiert und erläutert die Anforderungen des TÜV Rheinland Compliance-Management-System-Standards TR CMS 101:2015. Ziel des Leitfadens ist es, das Verständnis für die Standardanforderungen zu erhöhen und anhand zahlreicher Praxisbeispiele sinnvolle Anregungen für ihre unmittelbare Umsetzung zu geben.

Im Teil A dieses Leitfadens erhält der Leser eine Einführung in Zielsetzung, Struktur und die wichtigsten Merkmale des TR CMS 101:2015 – im Folgenden kurz TR CMS 101 genannt.

Im Teil B, dem Schwerpunkt des Leitfadens, werden dann die Anforderungen des Standards in Tabellenform stichwortartig aufgelistet und praxisorientiert interpretiert.

Mit Beispielen für die Dokumentation zum Nachweis der Erfüllung von Anforderungen soll dem Leser veranschaulicht werden, womit die Anforderungen belegbar sind.

Die dabei in der letzten Spalte der Tabelle angeführten Kennzahlen spiegeln die Möglichkeiten von Beispielen wider, die zur Messbarkeit und Steuerung von Compliance-Prozesse herangezogen werden können, um die Wirksamkeit des CMS ständig zu verbessern.

A TR CMS 101:2015 – eine Einführung

1 Allgemeines

1.1 Entstehung des Standards

Der TÜV Rheinland wurde im Jahr 2010 von Seiten seiner Kunden und von externen Beratern darauf aufmerksam gemacht, dass es am Markt keinen geeigneten, praxisorientierten und anwendbaren Standard zum Thema Compliance für Unternehmen und sonstige Organisationen gab. Dies veranlasste den TÜV Rheinland, sich mit der Thematik näher zu befassen, und das Ergebnis mündete im Frühjahr 2011 in die Erstellung und Veröffentlichung eines Zertifizierungsstandards für Compliance-Management-Systeme, des TR CMS 101. Somit war der Grundstein für ein zertifizierungsfähiges Compliance-Management-System gelegt.

1.2 Anwendung des Standards

Alle im TR CMS 101 festgelegten Anforderungen sind allgemeiner Natur (generisch) und auf alle Organisationen einschließlich öffentlicher Einrichtungen anwendbar, unabhängig von ihrer Art und Größe, der regionalen Ansässigkeit und der Art der bereitgestellten Produkte oder Dienstleistungen.

1.3 Ausschlüsse von Anforderungen

Der Standard ist so konzipiert, dass Ausschlüsse nicht vorgesehen sind. Da alle Forderungen unabhängig von der Struktur oder Größe der Organisation sind, können sie auch von kleinen Organisationen erfüllt werden. Alle Anforderungen der Standardkapitel 4–10 müssen demnach erfüllt sein, andernfalls kann keine Konformität bestätigt werden.

1.4 Bedeutung des Standards für Unternehmen und andere Organisationen

Die Erstellung, Einführung und Umsetzung eines Compliance-Management-Systems wird als eine präventive strategische Entscheidung einer Organisation verstanden. Dabei ist es wichtig, einen systematischen Nachweis eines gelebten Managementsystems, das zur Rechtskonformität der Organisation, seiner Aufsichtsorgane und Mitarbeiter beiträgt, führen zu können. Es ist für jede Organisation wichtig, darüber einen Nachweis führen zu können, dass bei einem Regelverstoß kein organisatorisches Verschulden vorlag. Mithilfe des TR CMS 101 wird das unternehmerische Risiko verringert. Da sich die regulatorischen Anforderungen auch in Anbetracht einer stetig fortschreitenden Globalisierung ändern und oftmals nicht nur nationale Gesetze greifen, ist es für Organisationen überlebenswichtig, mithilfe eines CMS diesen Anforderungen gerecht zu werden. Bei einigen Regelverstößen können die daraus folgenden Sanktionen unter Umständen die Existenz bzw. den Fortbestand der Organisation gefährden.

Organisationen können sich nach ihren organisatorischen Belangen und ihrem Umfeld ausrichten und sind frei in der Gestaltung ihres CMS. Der TR CMS 101 verlangt keine Vereinheitlichung von organisatorischen Strukturen, Prozessen oder Dokumentationen in den Orga-

nisationen; er gibt Hilfestellung und Orientierung für den systematischen Umgang mit einem CMS.

1.5 Die Sprache des Standards

Der TR CMS 101 ist international ausgerichtet und kann länderunabhängig angewandt werden. Deshalb ist er neben der deutschen auch in englischer Sprache veröffentlicht worden. Der Standard verwendet Begrifflichkeiten, die häufig aus dem Englischen stammen und im sonst üblichen Sprachgebrauch nicht vorkommen oder selten sind. Dies kann bei Neueinsteigern in die Thematik anfänglich zu gewissen Irritationen führen.

Im Folgenden einige der für den TR CMS 101 typischen Begriffe und ihre Synonyme:

- **Compliance** – Synonyme: Einhaltung, Befolgung, Konformität, Zustimmung etc. von/zu gesetzlichen und regulatorischen Vorgaben (Verbandsvorgaben, eigene unternehmensethische Vorgaben, Deutscher Corporate Governance Kodex etc.). Dies ist allgemeingültig und branchenunabhängig.
- **Organisation** – Synonyme: Unternehmen, Betrieb, Firma, öffentlich-rechtliche Einrichtung. Mit Organisation verbindet man im Deutschen allgemein eine Gruppierung von Personen, die keine Produkte herstellen.
- **Führung** (engl. top management) – Synonyme: Unternehmensleitung, Geschäftsführung, Behördenleitung
- **Leiten und Lenken** (engl. management bzw. to manage) – Synonyme: Hierfür sind im betrieblichen Sprachgebrauch i. d. R. andere Begriffe üblich, z. B. führen, organisieren, oder substantivische Begriffe wie z. B. Prozessführung oder schließlich auch „Management".
- **Lenkung** (engl. control) – Synonyme: Prüfung, Kontrolle, Führung.

In diesem Compliance-Leitfaden werden die o. g. Begriffe überwiegend wie in dem Standard verwendet.

2 Kompatibilität zu anderen Normen

Der TR CMS 101 hat strukturell eine große Kompatibilität zur ISO 19600 sowie zur ISO 9001 und folgt dem Managementansatz von Deming, dem Deming-Kreis: Planen, Durchführen, Überprüfen und Verbessern. Dieser Regelkreisansatz ist die Grundlage eines jeden Managementsystems. Damit kann jede Organisation auf gesetzliche und regulatorische Veränderungen reagieren und die Prozesse in der Organisation anpassen. Dem Leser wird auffallen, dass der TR CMS 101 auch Überlappungspunkte zu weiteren Normen aufweist. Dies macht gleichzeitig deutlich, dass Compliance eine Querschnittsfunktion in Organisationen darstellt und alle Bereiche tangiert. Damit wird aber auch deutlich, dass sich einzelne Normen wie z. B. ISO 14001, ISO 27001, ONR 49001 etc. in Teilbereichen zwar auch auf gesetzliche Vorgaben beziehen, aber nicht gänzlich alle gesetzlichen und regulatorischen Vorgaben, die für eine Organisation relevant sind, berücksichtigen können.

3 Grundsätze des Compliance-Managements

Zur Sicherstellung der originären Geschäftsziele müssen alle Organisationen unabhängig von der Branche, der Größe, ob im Inland oder auch im Ausland ansässig, den jeweiligen gesetzlichen und regulatorischen Vorgaben nachkommen. Dies regelt sich nicht von selbst, sondern bedarf gewisser organisatorischer Vorgaben und Maßnahmen, die in den einzelnen Organisationsprozessen umzusetzen sind. Der TR CMS 101 beschreibt in seinen einzelnen Kapiteln, welche Vorgaben erforderlich sind, um ein transparentes und effektives CMS zu erfüllen. Dabei soll die Angemessenheit für die jeweilige Organisation berücksichtigt werden. Darüber hinaus macht die Justiz bei der Verfolgung von Gesetzesverstößen im Allgemeinen keinen Unterschied hinsichtlich der Art und Größe der Organisation, es sei denn, das Gesetz lässt Ausnahmen zu.

Im Folgenden sind die Grundsätze zusammengefasst, die sich aus den Vorgaben des TR CMS 101 ergeben:

1) Compliance-Kultur

   Die Compliance-Kultur stellt die wesentliche Grundlage für jede Organisation dar. Dies bedeutet, dass die Führung durch aktives Vorleben erst die Voraussetzungen für das Annehmen, die Beachtung und das Umsetzen der Compliance-Vorgaben durch die Mitarbeiter oder sonstigen Organisationsangehörigen schafft.

2) Führung

   Führungskräfte haben eine Vorbildfunktion und müssen sich zur Einhaltung gesetzlicher, regulatorischer und ggf. auch eigener ethischer Vorgaben verpflichten und dies durch entsprechendes Verhalten vorleben. Genauso strikt müssen sie dies auch von ihren Mitarbeitern oder sonstigen Organisationsangehörigen einfordern.

3) Einbeziehung der Mitarbeiter

   Auf allen Ebenen werden Mitarbeiter im täglichen Arbeitsleben mit gesetzlichen Anforderungen direkt oder indirekt konfrontiert. Oftmals ist es dem Einzelnen nicht immer bewusst, dass seine Tätigkeit gesetzlichen Vorgaben genügen muss. Diesbezüglich ist eine Sensibilisierung der Mitarbeiter erforderlich. Sie sind es, die zum überwiegenden Teil die gesetzlichen Vorgaben im Unternehmen oder in Organisationen berücksichtigen und umsetzen bzw. einhalten müssen.

4) Administration des Compliance-Systems durch den Compliance-Beauftragten

   Jedes funktionierende System bedarf eines gewissen administrativen Aufwands, damit wesentliche überwachende Aufgaben, steuernde Aktivitäten sowie Auswertungs- und Berichterstattungstätigkeiten vollzogen werden. Dies geschieht nicht von selbst, daher ist eine Stelle erforderlich, die diese Funktionen und Aufgaben wahrnimmt, der Compliance-Beauftragte.

5) Compliance-Risikoanalyse

   Ohne eine Standortbestimmung wird es jeder Organisation schwerfallen, die richtigen Entscheidungen zu treffen. Dies gilt umso mehr, wenn es um Gesetzeskonformität geht. Die Organisation muss sich einen Überblick über ihr organisatorisches Umfeld (Rechtsform der Gesellschaft bzw. Organisation, Produkte,. Dienstleistungserbringung bzw. sonstige Aufgabenerfüllung, nationales oder internationales Agieren etc.) verschaffen, um die sich daraus ergebenden Compliance-Risiken richtig zu bewerten. Nur wenn man sich der Risiken bewusst ist, kann man dementsprechende Vorkehrungen zur Vermeidung

bzw. zur Minderung der Compliance-Risiken treffen. Diese Vorkehrungen müssen dann in die entsprechenden Prozesse und Arbeitsabläufe integriert werden.

6) Systemorientierter Managementansatz

Ermitteln, Verstehen, Leiten und Lenken von miteinander in Wechselbeziehung stehenden Prozessen als Systemansatz tragen zur Wirksamkeit und Effizienz ihrer Compliance-Ziele bei. Compliance sollte kein Zufallsprodukt, sondern ein Ergebnis von klaren Vorgaben und deren Umsetzung sein. Nur ein systematischer Ansatz, z. B. dem Deming-Kreis folgend, der eine Transparenz der Vorgaben und der Nachweise garantiert, ist belastbar und kann zur Entlastung der Organisation und der Führung herangezogen werden.

7) Systemüberwachung, -analyse und -verbesserung

Die ständige Verbesserung der Gesamtleistung der Organisation stellt ein permanentes Ziel der Organisation dar. Dazu wird das Compliance-Management-System durch verschiedenste Maßnahmen, wie z. B. durch

interne Compliance-Audits,

Tests der internen Kontrollen (gesetzte Maßnahmen oder Einrichtung zur Erkennung von Compliance-Verstößen) oder

Überwachung durch externe Prüfer/Prüfstellen

analysiert.

Diese Analyse aller verwertbaren Informationen sollte dann zur Verbesserung des Compliance-Management-Systems genutzt werden. Letztlich sollte jede Organisation das Ziel anstreben, Compliance-Verstöße zu verhindern und durch entsprechende Maßnahmen einen Schaden für die Organisation oder die Gesellschaft so gering wie möglich zu halten.

4 Wichtige Aspekte zur wirksamen Umsetzung des CMS

Dabei sind insbesondere folgende Aspekte zu überprüfen:

- Verpflichtung des Managements und der Mitarbeiter zur Einhaltung der Compliance-Vorgaben
- Schaffung und Etablierung einer Compliance-Kultur
- Regelmäßige Compliance-Risikoüberprüfung und -bewertung
- Aktualisierung der Rechtskataster und sonstiger compliance-relevanter Vorgaben
- Aktualisierung der Vorgabedokumente/Nachweisdokumente
- Ermittlung des Schulungsbedarfs und des Nachweises von Schulungen aller Mitarbeiter
- Nachweis von ausreichenden Ressourcen zur Umsetzung und Einhaltung von Compliance-Vorgaben
- Darlegung der Wirksamkeit des CMS durch: interne Audits, Überprüfung der installierten Kontrollen, Auswertung des Hinweisgebersystems, Umgang mit Compliance-Verstößen, regelmäßiges Compliance-Berichtswesen, Compliance Management Reviews etc.
- Festlegung und Verfolgung von Korrektur- und Vorbeugemaßnahmen zur Verbesserung des CMS

- Betrachtung der Prozesslandschaft

Ein nachhaltiges CMS kann durch die Anwendung der vorangegangenen Maßnahmen erreicht werden. Dies gibt allen Beteiligten eine gewisse Sicherheit, dass das Unternehmen bzw. die Organisation und seine bzw. ihre Partner sich rechtskonform verhalten und auch zukünftig durch eine systematische Vorgehensweise darauf geachtet wird, dass alle sich rechtskonform verhalten werden. Compliance schafft somit auch Planungssicherheit und Transparenz.

5 Nachhaltiger Erfolg durch Einbindung bereits vorhandener Managementsysteme

Der Zweck des Standards TR CMS 101 besteht darin, gesetzliche und regulatorische Anforderungen, soweit für die Organisation anwendbar, zu berücksichtigen und in einer systematischen und nachvollziehbaren Art und Weise zu definieren. Daraus lässt sich eine Handlungsanleitung für die Führung zur Einführung eines CMS ableiten. Dies führt bei richtiger Implementierung zu einer größeren Rechtssicherheit für die Organisation, für das Management, für die Mitarbeiter sowie für die externen Interessengruppen wie z. B. Aktionäre, Anteilseigner, Kunden, Lieferanten und sonstige interessierte Parteien. Dabei ist es wichtig, die Mitarbeiter diesbezüglich zu sensibilisieren und zu schulen. Da die meisten Organisationen für gewöhnlich schon Managementsysteme (wie z. B. ISO 9001, ISO 14001, ISO 27001 etc.) implementiert haben, können sie auf Teile dieser Managementsysteme zurückgreifen und auf sie referenzieren. Dies bedeutet, dass z. B. die Verwaltung und Aktualisierung der Dokumentation nicht unbedingt neu aufgesetzt werden muss oder bereits bestehende Prozess-, Verfahrens-, Arbeits-, Prüfanweisungen nicht extra für das CMS neu geschrieben werden müssen. Im CMS kann auf bereits bestehende Anweisungen referenziert werden, wenn diese als Vorgabe und zum Nachweis von Compliance-Forderungen geeignet sind. Für diejenigen Organisationen, die noch kein dokumentiertes Managementsystem implementiert haben, gibt der TR CMS 101 die aus anderen Normen bekannten Dokumentationsanforderungen vor. Genauso wie die einschlägig bekannten Normen zum Qualitätsmanagement, zum Umweltmanagement, zur Informationssicherheit, zum Arbeitsschutz etc. hat auch der TR CMS 101 eine präventive Ausrichtung. Dabei hat der Begriff der Prävention im Bereich Compliance noch einen brisanteren Charakter als in anderen Bereichen, weil hier alle anwendbaren gesetzlichen Anforderungen dahinterstehen und Verstöße juristische Sanktionen nach sich ziehen können. Dies kann bis zur privaten Haftung der involvierten Personen gehen. Aus diesem Grund sollte der Standard dazu genutzt werden, nachzuweisen, dass nicht nur eine partielle Compliance wie in den schon erwähnten ISO-Normen von der Organisation betrachtet wird, sondern dass dem TR CMS 101 folgend eine ganzheitliche Compliance betrieben wird.

6 Belastbare Nachweisführung

Der Umfang der Compliance-Dokumentation soll sich in angemessener Weise an der Größe der Organisation, der Komplexität der Prozesse, Produkte/Dienstleistungen und der Kompetenz der Mitarbeiter orientieren. Aus diesem Grund fordert der TR CMS 101 als Mindestumfang folgende Inhalte:

- Beschreibung der Compliance-Richtlinie (Corporate Governance, Code of Conduct)
- Beschreibung der Lenkung von Vorgabe- und Nachweisdokumenten

- Festlegung der Verantwortungen und Befugnisse z. B. durch Ernennung eines Compliance-Beauftragten
- Berichtswesen und Systembewertung
- Schulung, Sensibilisierung und Bewusstsein der Mitarbeiter
- Beschreibung der Compliance-Prozesse wie z. B. Compliance-Risikoanalyse, Beschreibung von Compliance-Anforderungen, Freigabeprozessen und Funktionstrennung, Hinweisgebersystem, Umgang mit compliance-relevanten Vorfällen (Verstößen) etc.
- Interne Audits
- Korrekturmaßnahmen
- Vorbeugemaßnahmen

Die Dokumentation dieser Anforderungen ist erforderlich, um einen gewissen Nachweis führen zu können, der belegt, dass die Organisation und die Führung nach den anerkannten Regeln der Technik bzw. dem aktuellen Stand des Wissens gehandelt haben. Es ist wichtig, einen Nachweis darüber führen zu können, dass die Organisation und die Führung sich keiner Fahrlässigkeit oder gar groben Fahrlässigkeit schuldig gemacht haben, da andernfalls existenzbedrohende Konsequenzen eintreten können. Die Organisation und ihre Führung sollten Auswirkungen dieser Art vermeiden.

B Tabelle „Interpretation der Anforderungen“

Um den Anwender des Standards bei der Umsetzung der Anforderungen in der Praxis und bei der Vorbereitung und Durchführung interner Audits zu unterstützen, werden in der folgenden Tabelle die einzelnen Normanforderungen interpretiert und durch nützliche Informationen ergänzt. Dabei wird ein durchgängiges Spaltenschema angewendet:

Standardanforderungen TR CMS 101:2015	Interpretation/ Aktivitäten	Dokumentationsbeispiele/ Nachweise	Beispiele für Kennzahlen

Erläuterungen zu den Tabellenspalten

1 Standardanforderungen TR CMS 101:2015

Die Anforderungen werden stichwortartig und nicht im Wortlaut aufgeführt. Das erleichtert die Arbeit in der Praxis, ersetzt allerdings nicht die Kenntnis des Originaltextes des Standards.

2 Interpretation/Aktivitäten

In dieser Spalte wird erläutert, was unter der Anforderung zu verstehen ist bzw. welche Aktivitäten beispielsweise zur Umsetzung der Anforderung in der Praxis zu ergreifen sind.

3 Dokumentationsbeispiele/Nachweise

Diese Spalte enthält Beispiele für Nachweisdokumente, die die Erfüllung der Standardanforderungen nachvollziehbar machen.

4 Beispiele für Kennzahlen

In dieser Spalte sind praxisnahe Kennzahlenbeispiele aufgelistet. Diese Beispiele sind Orientierungshilfen, die keinen Anspruch auf Vollständigkeit erheben.

Standardkapitel 4: Kontext der Organisation

Standardanforderung TR CMS 101:2015	Interpretation/ Aktivitäten	Dokumentationsbeispiele/ Nachweise	Beispiele für Kennzahlen
4.1 Verständnis der Organisation und ihres Kontexts **4.2 Verständnis der Bedürfnisse und Erwartungen interessierter Parteien**			
• Compliance-Umfeldanalyse • Verfahren zur Compliance-Umfeldanalyse	• Identifikation der relevanten Compliance-Themengebiete und interessierter Parteien • Analyse der identifizierten Compliance-Themengebiete und interessierter Parteien	• Rechtskataster • Liste der identifizierten Compliance-Themengebiete und interessierten Parteien (Kunden, Shareholder, Öffentlichkeit, Verbände, Mitarbeiter, Behörden etc.) • Bericht zur Compliance-Analyse/ Bewertung	
4.3 Festlegung des Geltungsbereichs des Compliance-Management-Systems			
• Geltungsbereich bestimmen	Zu berücksichtigen sind: • die Größe und Struktur der Organisation, Art ihrer Tätigkeit • Regionen, in denen die Organisation tätig ist, • bereitgestellte Produkte, • angewendete Prozesse, • Umfeld, sich verändernde Erfordernisse, • spezifische Risiken der Organisation und • besondere Ziele der Organisation. • Identifikation der relevanten Compliance-Themengebiete • Analyse der identifizierten Compliance-Themengebiete • Bewertung der identifizierten Compliance-Themen	• Rechtskataster • Liste der identifizierten Compliance-Themengebiete • Bericht zur Compliance-Analyse/ Bewertung • Maßnahmenkatalog • Regelmäßige Berichterstattung neuer/geänderter Compliance-Themen an die GF	
4.4 Compliance-Management-System und Prinzipien guter Führung			
• Prozessidentifikation • Prozessabfolge und Wechselwirkungen • Prozesslenkung • Prozessressourcen • Prozessüberwachung • Prozessakzeptanz • Prozessverbesserung	Aufbau einer regelkonform orientierten Organisation durch • direkten Zugang der Compliance-Funktion zu den Führungsgremien (Vorstand, Geschäftsführung, Aufsichtsrat etc.) • Unabhängigkeit der Compliance-Funktion (Stabsstelle, keine Linienfunktion) • angemessene Ausstattung der Compliance-Funktion mit Kompetenzen und Ressourcen • Definition, Festlegung und Darstellung von angemessenen und verständlichen Prozessen, ihrer Abfolge und Wechselwirkung • Festlegung von Wirksamkeitskriterien • Einbeziehung von Art, Umfang und Lenkung ausgegliederter Prozesse mit dem Ziel der Verbesserung des Compliance-Management-Systems	• CMS-Handbuch/CMS-Leitlinie/ Compliance-Richtlinien • Corporate Governance • Stellen- und Funktionsbeschreibungen • Rechtskataster • Genehmigungskataster • Prozesse/Verfahrensanweisungen und andere mitgeltende Dokumente • Prozessablaufpläne • Managementreview • Maßnahmenpläne • Organigramme • Selbstbewertungen • Analysepläne • Prüfpläne/Prüfberichte	

Standardanforderung TR CMS 101:2011	Interpretation/ Aktivitäten	Dokumentationsbeispiele/ Nachweise	Beispiele für Kennzahlen
4.5 Compliance-Verpflichtungen			
4.5.1 Identifizierung von Compliance-Verpflichtungen			
• Gesetze/behördliche Anforderungen und Verpflichtungen identifizieren • Compliance-Anforderungen analysieren und identifizieren • Auswirkungen der Compliance-Anforderungen auf die eigene Organisation feststellen • Bereitstellung und Kommunikation der aktuellen und gültigen Compliance-Anforderungen	• Kenntnis aller relevanten Compliance-Anforderungen und Verpflichtungen – Gesetze und Verordnungen – Regeln oder Leitlinien von Regulierungsbehörden – Urteile von Gerichten oder Verwaltungsgerichten – Abkommen mit Kommunen – Verträge mit Behörden und Kunden – Organisationsanforderungen wie Richtlinien und Verfahren – Freiwillige Grundsätze oder Verhaltenskodizes, Umweltverpflichtungen – Industriestandards • Verbreitung der Compliance-Anforderungen bei den betroffenen Stellen und Mitarbeitern • Erstellung einer Übersichtsliste der relevanten Compliance-Anforderungen • Compliance-Anforderungen liegen als gelenkte Dokumente vor	• Prozess-/Verfahrensbeschreibung • Rechtskataster • Liste der Adressaten für Compliance-Anforderungen • Compliance-Liste/Bericht zu den Auswirkungen für die Organisation • Aktualisierungsprotokolle	
4.5.2 Aufrechterhaltung und Aktualisierung von Compliance-Verpflichtungen			
• Compliance-Anforderungen analysieren und identifizieren • Auswirkungen der Compliance-Anforderungen auf die eigene Organisation feststellen • Bereitstellung und Kommunikation der aktuellen und gültigen Compliance-Anforderungen	• Kenntnis und regelmäßige Aktualisierung aller relevanten Compliance-Anforderungen und Verpflichtungen • Verbreitung der Compliance-Anforderungen bei den betroffenen Stellen und Mitarbeitern • Erstellung einer Übersichtsliste der relevanten Compliance-Anforderungen	• Prozess-/Verfahrensbeschreibung • Rechtskataster • Compliance-Liste/Bericht zur Aktualisierung der Compliance-Verpflichtungen	
4.6 Identifizierung, Analyse und Bewertung von Compliance-Risiken			
• Compliance-Umfeldanalyse • Compliance-Risiken • Compliance-Prozesse	• Identifikation der relevanten Compliance-Themengebiete • Analyse der identifizierten Compliance-Themengebiete • Bewertung der identifizierten Compliance-Themen • Erkenntnisse aus Compliance-Verstößen • Einleitung angemessener Vorbeugungsmaßnahmen • Regelmäßige Berichterstattung neuer/geänderter Compliance-Risiken an die Führung (Vorstand, GF etc.)	• Rechtskataster • Liste der identifizierten Compliance-Themengebiete • Bericht zur Compliance-Analyse/ Bewertung • Maßnahmenkatalog • Compliance-Risikobericht	• Sanktionskosten Bußgelder, Strafgelder, Auflagen etc. • Anzahl der Anzeigen/Beschwerden • Anzahl der Verstöße/versuchten Verstöße